Arizona Department of Veterans' Services

Information Technology Packet

ARIZONA DEPARTMENT OF VETERANS' SERVICES

INTERNAL MANAGEMENT POLICY 00-02

SUBJECT: INTERNET USAGE

EFFECTIVE DATE: September 18, 2003 (Supersedes July 1st, 2000)

1.0 POLICY: It is the policy of the Arizona Department of Veterans' Services (ADVS) to provide employees with Internet access and guidance on its use. The Internet is a communications tool made available to selected ADVS employees to enhance performance of their duties. Its use should be managed by rules of conduct applicable to any other Information Technology (IT) resource.

2.0 AUTHORITY: A.R.S. § 41-604, Duties and powers of the (ADVS) director; § 41-3504.A.1.(13), Powers and duties of the (GITA) agency; violation; classification; and § 41-1350, Records definition.

3.0 RESPONSIBILITY: Internet users shall comply with all applicable federal and state laws, including A.R.S. § 38-448, ADVS policies, procedures and guidelines. The IT Section is responsible for providing education on Internet use and giving employees acknowledgement forms to be signed. Supervisors are responsible for notifying the IT Section when employees require Internet access and collecting signed acknowledgement forms from employees. The ADVS Human Resources Section is responsible for filing acknowledgements in the official personnel file. Violation of this policy may result in revocation of the privilege to access the Internet and/or disciplinary action.

4.0 DEFINITIONS:

4.0 "Information Technology (IT)" means all computerized and auxiliary automated information processing, telecommunications and related technology, including hardware, software, vendor support and related services, equipment and projects.

4.1 "IT Section" means the ADVS office responsible for all aspects of IT for the agency (including Internet access for the agency).

4.2 "Human Resources Section" means the ADVS office responsible for all aspects of Human Resource issues for the agency.

4.3 "Internet" means an electronic communications network that connects computer networks and organizational computer facilities around the world.

4.4 "Internet user" means an agency employee, contract employee or other agency-authorized person who accesses the Internet through the use of state/agency owned/controlled computer equipment.

5.0 PROCEDURES:

5.0 Internet access is an IT/computer service and is the property of ADVS and the State of Arizona. ADVS reserves the right to monitor Internet use by any user at any time. The ADVS director or IT manager may determine

appropriate use and deny, revoke, suspend or close any user account at any time, based upon a determination of inappropriate use.

5.1 Employees who have a personal computer at their work site may, with appropriate supervisory permission, have access to the Internet. Access is primarily intended as a business tool for conducting authorized state activities. Examples of business related Internet use include, but are not limited to:

5.1.1 Communications and information exchanges directly relating mission, goals and work tasks of ADVS.
5.1.2 Announcements of state laws, procedures, hearings, policies, services or activities.
5.1.3 Use for advisory, standards, research, analysis, and professional society or development activities related to the user's departmental duties and responsibilities.
5.1.4 Ordering products through a business web site in accordance with procurement procedures.

5.2 ADVS believes appropriate use of the Internet can enhance the quality of an employee's work experience and is conducive to increased productivity while at work. ADVS encourages employees to make judicious use of this unique tool and recognizes employees may need to access the web for personal business, similar to using the telephone. ADVS expects employees to be engaged in work-related tasks during their assigned duty hours. Private use of the Internet only should occur during breaks, lunch periods or off-duty periods before or after work. Some examples of acceptable private use include, but are not limited to:

5.2.1 Increasing knowledge of, and familiarity with, the Internet through use and practice.
5.2.2 Conducting business with government entities such as registering an automobile with the Motor Vehicle Division of the Arizona Department of Transportation.
5.2.3 Maintaining contact with business organizations such as news bureaus or organizations.
5.2.4 Research and study.
5.2.5 Using e-mail to maintain personal correspondence.

5.2.5.1 Personnel should not use the ADVS internal E-mail system for personal use. If a user wishes to send personal correspondence, Internet based E-mail systems such as Hotmail, Yahoo and the like should be utilized instead.
5.2.5.2 Internet E-mail is subject to the same restrictions and guidelines contained in the ADVS E-mail Usage IMP 00-01.
5.2.5.3 Users should not consider E-mail to be either private or secure.
5.2.5.4 E-mail via the Internet is not as reliable or as secure as

internal E-mail.

5.2.5.5 Internet E-mail users should be aware that ADVS monitors Internet use, including sites visited, without user consent and without prior notice.

5.2.5.6 Employees wishing to check personal E-mail accounts (e.g., Hotmail, Yahoo, or web mail from their ISP [Internet Service Provider]) using ADVS equipment should think about the content of any E-mail in their personal accounts prior to accessing it. If any content includes rude or offensive language, nudity or depictions of nudity, or sexual content, it should not be accessed.

5.2.6 The use of Streaming Audio or Video such as Real Player or Windows Media Player for personal use is discouraged between the hours of 0600 and 1700. Streaming Audio and Video tends to slow down Internet connection for the site as well as slow response times on network applications.

5.2.7 The use of personal "thumb drives", flash drives, digital media cards or any other personal digital media is strictly prohibited.

5.3 It is unacceptable for an Internet user to view, submit, publish, display, or transmit on the network, or any ADVS computer system, any information that:

5.3.1 Violates or infringes on the rights of any other person.

5.3.2 Contains defamatory, false, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.

5.3.3 Contains rude or offensive language, nudity or depictions of nudity, or any type of sexual content, or ultimate sex acts (as defined in Title 38, ARS § 38-448).

5.3.4 Violates any applicable federal, state or agency regulations prohibiting sexual harassment.

5.3.5 Intentionally restricts or inhibits other authorized users from using the system or the efficiency of the computer systems.

5.3.6 Encourages the use of controlled substances or uses the system for the purpose of criminal intent.

5.3.7 Uses the system for any other illegal purpose.

5.3.8 Solicit any activity prohibited by law.

5.3.9 Transmit material, information, or software in violation of any local, state, or federal law.

5.3.10 Conduct any political activity.

5.3.11 Conduct any gambling, betting or gaming activity.

5.3.12 Conduct any activity for personal gain (e.g., stock trading).

5.3.13 Make unauthorized purchases.

5.4 Consent – All Internet users shall acknowledge and consent that all Internet, network and Information Systems activity is the property of ADVS and the State of Arizona, and therefore, should not consider any Internet activity to be private.

5.4.1 The IT Section is authorized to monitor all Internet traffic and to use tracking software, or other state agencies/independent contractors for the purpose of monitoring Internet traffic. Any violations will be reported to the appropriate supervisor for disciplinary action.

5.4.1.1 IT Section personnel are authorized to view material deemed unauthorized in section 5.3 of this policy for the purposes of monitoring and verification.

5.4.2 The IT Section understands accidents can happen. If there is a situation where an employee accidentally clicks on an Internet link that brings up an inappropriate website, the employee should immediately report in writing to his/her supervisor the situation including the name of the site viewed and time of access.

5.5 Copyright laws must be obeyed. All communications and information accessible via the Internet should be assumed to be private property. Internet users shall honor copyright laws, including those protecting software and intellectual property.

5.5.1 Duplicating, transmitting, or using software not in compliance with software license agreements is considered copyright infringement.

5.5.2 Users shall not make copies of software or literature without proper authorization and the full legal right to do so.

5.5.3 Unauthorized use of copyrighted materials, or another person's original writings, is considered copyright infringement.

5.5.4 Internet users shall not transmit copyrighted materials, belonging to others, over the Internet without permission.

5.5.5 If ADVS permits, users may download copyrighted material from the Internet, but its use must conform to the restrictions posted by the author or current copyright law.

5.5.6 Copyrighted information used on web sites must be clearly identified as such.

5.5.7 Public domain material may be downloaded for business related use. Redistribution of public domain materials is done so with the assumption of all risks regarding the determination of whether or not the materials are in the public domain. Any redistribution of public domain materials is strictly limited to non-commercial use.

5.5.8 The use of peer-to-peer file sharing applications such as Kazaa, Morpheus, iMESH and similar programs is strictly prohibited.

5.6 Downloading – Downloading information from the Internet is permitted only when it meets the restrictions of the ADVS director or IT Manager.

5.6.1 If a user's downloaded material may have been infected by a virus, the user should contact the IT Section immediately.

5.6.2 The use of screensaver programs, mouse pointer programs, and other desktop enhancing software is not allowed. These programs may allow for additional backgrounds, screensavers, cursors, etc., but they can affect the performance of the computer. Examples of this software include Webshots, Comet Cursor, Bonzi Buddy, etc.

If an IT Section staff member deems any of the downloaded software to be adversely affecting the performance of the PC, the IT Section staff member shall be authorized to remove the software and immediately notify the employee's supervisor. Once removed, the software is prohibited from re-installation. If the employee re-installs the software, the IT Section shall inform the employee's supervisor for disciplinary action.

5.6.3 The use of photographs as wallpaper is authorized, however, as with any other office display, employees should use good judgment and taste in placing these items on their computers.

5.6.4 Many kinds of software are available through the Internet. Virus free, shareware, freeware or other software may be used when approved by the IT Section. Copyright laws shall be observed at all times.

5.7 Records retention of electronic information is outlined in the ADVS E-mail Usage IMP 00-01.

5.7.1 The records retention requirements shall apply to all records obtained or received via the Internet.

5.7.2 ADVS employees who transmit or receive material via the Internet shall determine whether to preserve or delete the material and communication's consistent with the records retention schedule and records retention policy of ADVS.

5.8 ADVS employees with questions regarding records retention should contact the IT Section and/or review ARS §§ 41-1347, 41-1350, and 39-121.01(B).

5.8.1 Routine E-mail and communications (similar to oral conversation and voice mail, defined as expeditious communication on routine matters such as scheduling meetings and conference calls) may be deleted after the required action is taken.

5.9 Regulation and policy enforcement is ultimately the responsibility of the ADVS director.

5.9.1 The IT Section manager shall be responsible for agency compliance with the provisions of this policy and for investigating suspected incidents of non-compliance.

5.9.1.1 IT Section personnel are authorized to view material deemed unauthorized in section 5.3 of this policy for the purposes of monitoring and verification.

5.9.2 If in doubt, Internet users should seek policy clarification from an appropriate ADVS supervisory authority. Agency employees with questions regarding records retention should contact their supervisor and refer to A.R.S. §§ 41-1347, 41-1350, and 39-121.01(B).

6.0 IMPLEMENTATION: This policy shall be implemented without change on the effective date.

_____

Patrick F. Chorpenning, Director

ARIZONA DEPARTMENT OF VETERANS' SERVICES

INTERNAL MANAGEMENT POLICY 00-01

SUBJECT: E-MAIL USAGE

EFFECTIVE DATE: September 18, 2003 (Supersedes July 1st, 2000)

1.0 POLICY: It is the policy of the Arizona Department of Veterans' Services (ADVS) to provide guidance on the proper use, preservation, disclosure and disposition of electronic mail. This policy, based on state law, describes the legitimate use of electronic mail with special emphasis on records-related issues.

2.0 AUTHORITY: A.R.S. § 41-604, Duties and powers of the (ADVS) director; § 41-3504.A.1.(13), Powers and duties of the (GITA) agency; violation; classification; and § 41-1350, Records definition.

3.0 RESPONSIBILITY: E-mail users are responsible for complying with this policy and attending annual E-mail training. The Information Technology (IT) Section is responsible for providing education on E-mail use and giving employees acknowledgment forms to be signed. Supervisors are responsible for notifying the IT Section when employees require initial training and collecting signed acknowledgments from employees. ADVS' Human Resources Section is responsible for filing acknowledgments in employees' personnel files. Violation of this policy may result in revocation of E-mail privileges and/or disciplinary action.

4.0 DEFINITIONS:

4.1 "E-Mail" means a communications tool (Electronic-mail) made available to certain agency employees for the performance of their duties. The purpose of E-mail is to provide expeditious communication among ADVS employees similar to oral conversation and voice mail.

4.2 "E-mail User" means an agency employee, contract employee or other agency-authorized person who accesses E-mail through the use of state/agency owned/controlled computer equipment.

4.3 "GITA" means Government IT Agency, the agency responsible for providing state agencies statewide guidelines on IT.

4.4 "Information Technology (IT)" means all computerized and auxiliary automated information processing, telecommunications and related technology, including hardware, software, vendor support and related services, equipment and projects.

4.5 "IT Section" means the ADVS office responsible for all aspects of IT for the agency (including E-mail accounts for agency personnel).

4.6 "Human Resources Section" means the ADVS office responsible for all aspects of Human Resource issues for the agency.

7.0 PROCEDURES: The IT Section manager shall be responsible for agency compliance with the provisions of this policy and for investigating suspected incidents of non-compliance. If in doubt, E-mail users should seek policy clarification from their direct supervisor or the IT Section.

7.0 E-mail users are responsible for complying with the following usage requirements in receiving/sending/maintaining E-mail messages:

7.0.1 Personnel should not use the ADVS internal E-mail system for personal use. If a user wishes to send personal correspondence, Internet based E-mail systems such as Hotmail, Yahoo and the like should be utilized instead.

7.0.2 All state employees with access to E-mail must acknowledge and consent that all network activity is the property of ADVS and the State of Arizona, and therefore, should not consider any E-mail activity to be private.

7.0.3 E-mail communications shall be professional in content; appropriate to a government agency; in compliance with agency and statewide policy; and consistent with other agency policies and procedures.

7.0.4 Agency work rules governing use of State property, record keeping and communications with others also apply to the use of E-mail. Users should never send an E-mail communication they would not feel comfortable communicating face-to-face or over the phone.

7.0.5 No E-mail communications shall be created or sent that might constitute discriminatory, harassing, intimidating, hostile or offensive communications based on gender, race, color, national origin, sexual orientation, disability, or other grounds.

7.0.6 Employees shall not read the E-mail of another employee without a legitimate business purpose consistent with the agency's policies and business communications practice.

7.0.7 No employee shall send E-mail under another person's name without that person's authorization, and the sender shall indicate his or her identity in the message.

7.0.8 Employees shall follow all security policies of the agency as set forth in section 5.3 of this internal management policy.

7.0.9 Generally, employees shall be expected to use reasonable judgment in the performance of their duties. Failure to do so may subject them to disciplinary procedures consistent with the policies of the agency.

7.1 E-mail for personal use:

7.1.1 Personnel should not use the ADVS internal E-mail system for personal use. If a user wishes to send personal correspondence, Internet based E-mail systems such as Hotmail, Yahoo and the like

should be utilized instead.

7.1.2 Internet E-mail is subject to the same restrictions and guidelines as the ADVS Internet Usage IMP 00-02.

7.1.3 Users should not consider Internet based E-mail to be either private or secure.

7.1.4 Internet E-mail users should be aware ADVS monitors Internet use, including sites visited, without user consent and without prior notice.

7.1.5 Employees wishing to check personal E-mail accounts (e.g., Hotmail, Yahoo, or web mail from their ISP [Internet Service Provider]) using ADVS equipment should think about the content of any E-mail in their personal accounts prior to accessing it. If any content includes rude or offensive language, nudity or depictions of nudity, or sexual content, it should not be accessed.

7.2 E-mail is not secure. E-mail transmitted inside the agency is more secure than E-mail transmitted to state agencies on the Multiple Agency Network (MAGNET), and far more secure than E-mail transmitted via the Internet.

7.2.1 The agency may establish additional levels of security, ranging from password protection to authentication and encryption. The IT Section will work with supervisors to determine appropriate security levels for various E-mail accounts.

7.2.2 No Privacy in E-mail. Employees using E-mail shall have no expectation of privacy related to the use of this technology.

7.3 Ownership of E-mail. The E-mail accounts and the contents thereof are property of ADVS and the State of Arizona.

7.3.1 All messages created in the system belong to the State, not employees, vendors or customers.

7.3.2 The agency reserves the right to monitor E-mail use by any user at any time.

7.4 The E-mail user is responsible for determining which E-mail messages are records and which have no continuing value to the agency.

7.4.1 When an E-mail message is a record, then the E-mail message and related transmission and receipt data shall be retained in accordance with State statutes and approved records disposition schedules for the applicable record series. See section 5.7 below for additional information.

7.4.2 E-mail messages of only transitory value need not be saved. See section 5.7 below for additional information.

7.4.3 Agency management is responsible for creating and distributing E-mail records policies, appropriate to the agency's business needs and for implementing those policies, including training.

7.4.4 End users are responsible for managing E-mail messages they receive and properly identifying, classifying, retaining, and disposing of messages, in accordance with statewide and agency

policies, as well as the technical means at their disposal.

7.5 Unacceptable use of agency E-mail. E-mail shall not be used for the following purposes:

7.5.1 Personal business or personal gain without authorization.
7.5.2 Soliciting.
7.5.3 Political campaigning.
7.5.4 Unethical, illegal, unprofessional or disruptive activities.
7.5.5 Any activity that would jeopardize the legitimate interests of the State or the citizens and Veterans' of the State of Arizona.

7.6 E-mail records retention and disposition. E-mail may be used to facilitate routine matters such as scheduling meetings and conference calls; notification of legal and policy issues to be resolved in more formal communication; requests for information; or directives to complete tasks; and notification of employees' whereabouts (e.g., vacations, conference, and out-of-office).

7.6.1 Employees who transmit E-mail shall determine whether to preserve or delete the E-mail communication, as follows:

7.6.1.1 Routine E-mail, of transitory value, may be deleted after the appropriate action is taken. No paper or computer record need be preserved unless the communication is subject to retention under this policy.
7.6.1.2 Communication that meets the definition of a record under A.R.S § 41-1350, transmitted inside the agency, or received from outside the agency, through the E-mail system, shall be printed and preserved in the appropriate file, in permanent paper format **or** preserved, unedited, in the E-mail system without printing.
7.6.1.2.1 An excerpt from the statute that defines "record" reads, "made or received by any governmental agency in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government, or because of the informational and historical value of data contained therein."
7.6.1.2.2 With every communication that qualifies as a record, the sender shall, ensure that:
7.6.1.2.2.1 The time and date the message was sent and received; the complete sender and receiver identification, and; the complete message, are preserved.
7.6.1.2.2.2 The E-mail may be preserved as any

other type of record by being either printed out and preserved in the hardcopy file, **or** preserved in an electronic archive.

7.6.2 Communications subject to an existing public records request, or to formal discovery in ongoing litigation, will be preserved in the appropriate file or the E-mail system.

7.7 IT Section responsibilities relative to E-mail:

7.7.1 E-mail systems will be backed up regularly.

7.7.1.1 The E-mail data backup will be deleted pursuant to the Department of Library, Archives and Public Records' approved Records Disposition Schedule for the agency.

7.7.1.2 The IT Section will document its schedule for E-mail backup and provide a copy of the systems backup to GITA.

7.7.1.3 Periodic record of E-mail system address books and distribution lists will be retained pursuant to the Department of Library, Archives and Public Records' approved Records Disposition Schedule for the agency.

7.7.2 Employees will be provided with E-mail use policies.

7.7.2.1 New employees shall not be granted access to the E-mail system until they have received training.

7.7.2.2 E-mail training shall, at least once per year, be provided to all employees interested in attending.

7.7.3 ADVS shall, at least once per year, perform a random documented audit of employee E-mail use.

7.7.3.1 The audit shall, at a minimum, include review of E-mail messages transmitted and received by a reasonable percentage of E-mail users, to be determined by the ADVS director.

7.7.3.2 The IT manager may access E-mail, at any time, to ensure compliance with this policy.

7.7.3.3 Agency employees with questions regarding records retention should contact their supervisor and refer to A.R.S. §§ 41-1347, 41-1350, and 39-121.01(B).

7.7.3.4 If in doubt, Internet users should seek policy clarification from an appropriate ADVS supervisory authority.

6.0 IMPLEMENTATION: This policy shall be implemented without change on the effective date.

_____

Patrick F. Chorpenning, Director

ARIZONA DEPARTMENT OF VETERANS' SERVICES

INTERNAL MANAGEMENT POLICY 00-04

SUBJECT: CELLULAR (CELL) PHONE USAGE

EFFECTIVE DATE: October 3, 2003

1.0 POLICY: It is the policy of the Arizona Department of Veterans' Services (ADVS) to provide selected employees with cell phones and guidance on cell phone use. Cell phones are a communications tool made available to selected ADVS employees to enhance performance of their duties. Cell phone use should be managed by rules of conduct applicable to any other state resource.

2.0 AUTHORITY: A.R.S. § 41-604, Duties and powers of the (ADVS) director

8.0 RESPONSIBILITY: Cell phone users shall comply with all applicable federal and state laws, ADVS policies, procedures and guidelines. The ADVS Purchasing Office is responsible for providing education on cell phone use and giving employees acknowledgement forms to be signed. Supervisors are responsible for notifying the Purchasing Office when employees require a cell phone and collecting signed acknowledgement forms from employees. The ADVS Human Resources Section is responsible for filing acknowledgements in the official personnel file. Violation of this policy may resulting revocation of cell phone privileges and/or disciplinary action.

9.0 DEFINITIONS:

9.0 "Purchasing Office" means the ADVS office responsible for all aspects of Business related expenses for the agency (including Cell phone usage for the agency).

9.1 "Human Resources Section" means the ADVS office responsible for all aspects of Human Resource issues for the agency.

9.2 "Cell phone user" means an agency employee, contract employee or other agency-authorized person who has been assigned a cell phone from the state/agency owned/controlled equipment, or who uses a personal cell phone, for conducting authorized state activities.

10.0 PROCEDURES:

10.0 Cell phone usage is a service and the property of ADVS and the state of Arizona. ADVS reserves the right to monitor cell phone use by any user at any time. The ADVS director or Purchasing Office manager may determine appropriate use and deny, revoke, suspend or close any user account at any time, based upon a determination of inappropriate use.

10.1 Employees may, with appropriate supervisory permission, be issued a cell phone. Cell phone use should be primarily intended as a business tool for

conducting authorized state activities. Supervisors should contact the Business Office for all cell phone related issues.

10.1.1 Employees in possession of state-issued equipment such as cell phones are expected to protect the equipment from loss, damage or theft. Upon resignation or termination of employment, or at any time upon request, the employee may be asked to produce the cell phone for return or inspection. Employees unable to present the cell phone in good working condition within the time period requested (e.g., within 24 hours) may be expected to bear the full cost of replacement.

10.1.2 Employees contacted by personal creditors or collection agencies should immediately inform the caller of this policy and end the call. The employee shall inform personal creditors or collection agencies in writing advising them not to call the employee at work. Personal creditors or collection agencies who fail to honor such a request can be reported to the Federal Trade Commission at www.ftc.gov

10.2 Safety Issues for Cellular Phone Use

10.2.1 Employees whose job responsibilities include regular or occasional driving and who are issued a cell phone, or use their personal cell phone, for conducting authorized state activities, are expected to refrain from using the cell phone while driving. Safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees are strongly encouraged to pull off to the side of the road and safely stop the vehicle before placing or accepting a call. If acceptance of a call is unavoidable and pulling over is not an options, employees are expected to keep the call short, use hands-free options, if available, refrain from discussion of complicated or emotional discussions, and keep their eyes on the road. Special care should be taken in situations involving traffic, inclement weather, or unfamiliar surroundings.

10.2.2 In situations where job responsibilities include regular driving and accepting of business calls, hands-free equipment will be provided to facilitate the provisions of this policy. Contact the Business Office to facilitate the purchase of hands-free accessories.

10.2.3 Employees whose job responsibilities do not specifically include driving as an essential function, but who are issued a cell phone, or use their personal cell phone, for conducting authorized state activities, are also expected to abide by these provisions. Under no circumstances are employees allowed to place themselves at risk to fulfill business needs.

10.2.4 Employees who are charged with traffic violations resulting from the use of their cell phone while driving will be solely responsible for all

liabilities resulting from such actions.

10.3 ADVS recognizes employees may occasionally need to place and receive personal phone calls using a cell phone while on duty. In such cases, the length and frequency of personal calls should be kept to a minimum, whether or not the calls are placed and received using state-issued or personal cell phones. Receiving and placing excessive calls is disruptive to others. Therefore, abuse may result in revocation of cell phone privileges and/or disciplinary action. Personal cell phones and other communication devices that are not being used for authorized state activities are required to be kept in silent mode while employees are on duty.

10.3.1 Personal calls using state equipment shall not cause the state to incur any discernable cost or expense.

10.3.2 Personal phone calls during working hours distract employees from their job responsibilities and may be disruptive to coworkers. Therefore, employees shall limit the placing or receiving of personal calls while on duty to emergencies.

10.3.3 Personal calls should not interfere or have any noticeable negative impact upon the employee's performance of duties and provision of services.

10.3.4 Personal calls should not bring discredit or embarrassment to the state or agency.

10.3.5 Employees are expected to inform friends and family members of this policy and will be held accountable for their actions under the company's disciplinary procedures.

11.0 IMPLEMENTATION: This policy shall be implemented without change on the effective date.

_____

Patrick F. Chorpenning, Director

Title 38, ARS §38-448

Be it enacted by the Legislature of the State of Arizona:

Section 1. Title 38, chapter 3, article 4, Arizona Revised Statutes, is amended by adding section 38-448, to read:

38-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions

A. EXCEPT TO THE EXTENT REQUIRED IN CONJUNCTION WITH A BONA FIDE, AGENCY APPROVED RESEARCH PROJECT OR OTHER AGENCY APPROVED UNDERTAKING, AN EMPLOYEE OF AN AGENCY SHALL NOT KNOWINGLY USE AGENCY OWNED OR AGENCY LEASED COMPUTER EQUIPMENT TO ACCESS, DOWNLOAD, PRINT OR STORE ANY INFORMATION INFRASTRUCTURE FILES OR SERVICES THAT DEPICT NUDITY, SEXUAL ACTIVITY, SEXUAL EXCITEMENT OR ULTIMATE SEXUAL ACTS AS DEFINED IN SECTION 13-3501. AGENCY HEADS SHALL GIVE, IN WRITING, ANY AGENCY APPROVALS. AGENCY APPROVALS ARE AVAILABLE FOR PUBLIC INSPECTION PURSUANT TO SECTION 39-121.

B. AN EMPLOYEE WHO VIOLATES THIS SECTION PERFORMS AN ACT THAT IS CAUSE FOR DISCIPLINE OR DISMISSAL OF THE EMPLOYEE AND FOR AN EMPLOYEE IN STATE SERVICE IS CONSIDERED MISUSE OR UNAUTHORIZED USE OF STATE PROPERTY PURSUANT TO SECTION 41-770.

C. ALL AGENCIES SHALL IMMEDIATELY FURNISH THEIR CURRENT EMPLOYEES WITH COPIES OF THIS SECTION. ALL AGENCIES SHALL FURNISH ALL NEW EMPLOYEES WITH COPIES OF THIS SECTION AT THE TIME OF AUTHORIZING AN EMPLOYEE TO USE AN AGENCY COMPUTER.

D. FOR THE PURPOSES OF THIS SECTION:

1. "AGENCY" MEANS:

(a) ALL OFFICES, AGENCIES, DEPARTMENTS, BOARDS, COUNCILS OR COMMISSIONS OF THIS STATE.

(b) ALL STATE UNIVERSITIES.

(c) ALL COMMUNITY COLLEGE DISTRICTS.

(d) ALL LEGISLATIVE AGENCIES.

(e) ALL DEPARTMENTS OR AGENCIES OF THE STATE SUPREME COURT OR THE COURT OF APPEALS.

2. "INFORMATION INFRASTRUCTURE" MEANS TELECOMMUNICATIONS, CABLE AND COMPUTER NETWORKS AND INCLUDES THE INTERNET, THE WORLDWIDE WEB, USENET, BULLETIN BOARD SYSTEMS, ON-LINE SYSTEMS AND TELEPHONE NETWORKS.

APPROVED BY THE GOVERNOR APRIL 17, 2003.

FILED IN THE OFFICE OF THE SECRETARY OF STATE APRIL 18, 2003.

ARIZONA DEPARTMENT OF VETERANS' SERVICES

USER AFFIRMATION STATEMENT

EFFECTIVE DATE: October 1st, 2003

I have been made aware and understand that all personnel who have access to ADVS data, computers, E-mail and network resources are bound by applicable laws, rules and ADVS policies regarding. I agree to abide by all applicable laws, rules and ADVS policies, and I pledge to refrain from any and all of the following:

1. Revealing ADVS data to any person or persons outside or within ADVS who have not been specifically authorized to receive such data.
2. Attempting or achieving access to ADVS data not germane to my mandated job functions.
3. Entering/altering/erasing ADVS data maliciously or in retribution for real or imagined abuse, or for personal amusement.
4. Entering/altering/erasing ADVS data for direct or indirect personal gain or advantage.
5. Using ADVS terminals, printers, and/or other equipment inappropriately.
6. Using another person's personal ADVS logon ID and password.
7. Revealing my personal ADVS logon ID and password to any unauthorized personnel.
8. Asking another user to reveal his/her personal ADVS login ID and password.

In relation to my responsibilities regarding proprietary rights of the authors or computer software utilized by ADVS, I recognize that:

1. ADVS licenses the use of computer software from a variety of outside companies. ADVS does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce or alter the software or the documentation.
2. When used on a local area network or on multiple machines, ADVS employees shall use the software in accordance with the license agreement.
3. ADVS employees who know of any misuse of software or related documentation within the agency shall notify their manager/supervisor or the IT Section.
4. ADVS employees making, acquiring or using unauthorized copies of computer software are subject to disciplinary action in accordance with Internal Management Policy 00-02.
5. According to U.S. Copyright Law, 17 USC Sections 101 and 506, illegal reproduction of software can be subject to criminal damages up to $250,000 and/or up to 5 years imprisonment.
6. In the event that an employee is sued or prosecuted for the illegal reproduction of software, he/she will not be represented by ADVS or the Arizona Attorney General.

Appropriate action will be taken to ensure that applicable federal and state laws, regulations, and ADVS policies governing confidentiality and security are enforced. A breach of procedure occurring pursuant to this policy or misuse of department property including computer programs, equipment and/or data may result in disciplinary action, including dismissal, and/or prosecution in accordance with any applicable provision of law.

My signature below confirms that I have read and accept responsibility for adhering to all applicable laws, rules, regulations and ADVS policies. Failure to sign this statement will mean that I will be denied access to ADVS data, computer equipment and software.

Signature: _____ Date: _____

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

INTERNET USAGE POLICY ACKNOWLEDGEMENT FORM

EFFECTIVE DATE: October 1st, 2003

I, _____, have read and understand the Internet Usage Internal Management Policy 00-02 for the Arizona Department of Veterans' Services and been provided with a copy of A.R.S. § 38-448. I agree to comply with all terms and conditions of this policy and statute.

I also understand and agree that all Internet, network and information systems activity conducted with state/agency resources is the property of the Arizona Department of Veterans' Services and the State of Arizona.

I understand that the Arizona Department of Veterans' Services reserves the right to monitor and log all network activity, including Internet access, with or without notice. I have no expectation of privacy in the use of these resources.

Signed: _____

Date: _____

I agree that the above mentioned employee requires Internet access to complete their job function more efficiently.

Division Head: _____

Signed: _____

Date: _____

LIABILITY
The Arizona Department of Veterans' Services makes no warranties of any kind, whether express or implied, for the use of the Internet or electronic information resources. Additionally, the Arizona Department of Veterans' Services is not responsible for any damages whatsoever that employees may suffer arising from or related to use of the Internet or electronic information resources.

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

E-MAIL USAGE POLICY ACKNOWLEDGEMENT FORM

EFFECTIVE DATE: October 1st, 2003

I, _____, have read and understand the E-mail Usage Internal Management Policy 00-01 for the Arizona Department of Veterans' Services. I agree to comply with all terms and conditions of this policy.

I understand and agree that all Internet, network and information systems activity conducted with state/agency resources is the property of the Arizona Department of Veterans' Services and the State of Arizona.

I understand that the Arizona Department of Veterans' Services reserves the right to monitor and log all network activity, including E-mail, with or without prior consent or notice. I have no expectation of privacy in the use of these resources.

Signed:

_____Date:_____

LIABILITY

The Arizona Department of Veterans' Services makes no warranties of any kind, whether express or implied, for the use of the E-mail system or electronic information resources. Additionally, the Arizona Department of Veterans' Services is not responsible for any damages whatsoever that employees may suffer arising from or related to use of E-mail or electronic information resources.

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

CELL PHONE USAGE POLICY ACKNOWLEDGEMENT FORM

EFFECTIVE DATE: October 1st, 2003

I, _____, have read and understand the Cell Phone Usage Internal Management Policy 00-04 for the Arizona Department of Veterans' Services. I agree to comply with all terms and conditions of this policy. Violation of this policy may resulting revocation of the privilege and/or disciplinary action.
.

I understand cell phone usage is a service and is the property of ADVS and the State of Arizona. ADVS reserves the right to monitor Cell phone use by any user at any time. The ADVS Director or Purchasing Office manager may determine appropriate use and deny, revoke, suspend or close any user account at any time, based upon a determination of inappropriate use.

Signed:

_____Date:_____

LIABILITY

Employees who are charged with traffic violations resulting from the use of their phone while driving will be solely responsible for all liabilities that result from such actions.

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

MDI ACCESS REQUEST FORM

(FOR USE ONLY WHEN MDI ACCESS IS REQUIRED)

EFFECTIVE DATE: October 1st, 2003

Check One:

□ New Employee Date of hire: _____

□ Reset Password

□ End of Employment Date of release: _____

Employee Details: (print clearly)

First Name: _____ Last Name: _____

Job Title: _____

Location: _____

Unit Supervisor:_____ Is MDI Access Needed (circle one) Yes No

Unit Supervisor Signature_____

Discipline: (Check only one)

□ Accounting
□ Accounts Payable
□ Accounts Receivable
□ Activity Director
□ Administrator
□ All Disciplines
□ Care Plan Coordinator
□ CEO
□ CFO
□ Charge Nurse
□ CMT
□ D.O.N / A.D.O.N.
□ Dietary
□ Dietary Supervisor
□ Director of Nursing
□ General Ledger
□ Human Resources
□ LPN
□ Medical Secretary
□ Nursing Assistant
□ Payroll
□ Restorative Aide
□ RN
□ Social Services

MDI Application Access:

□ Accounts Receivable (complete page 2 sec. A)

□ Clinical Care (Medical Records (complete page 2 sec. B)

□ Schedule Pro

□ Copy (Duplicate) Access Permissions From Employee: _____

□ Remove All MDI Access

Specify Employee work hours for MDI access:

Start time: _____ End time: _____ OR □ Rotating schedule, 24 hr access

Submitted by: _____ (please print) Title: _____

MDI Access needed: □ ASAP or By Date: _____

Sec. A
Accounts Receivable Limited Access

Unchecked boxes will deny access. Checked boxes allows access.

- □ Resident File Maintenance
- □ Enter Billing Transactions
- □ Resident Census Billing
- □ Resident Inquiry
- □ Classification Maintenance
- □ Ancillary Maintenance
- □ Resident Statements
- □ Month End Recap
- □ Aging Report
- □ Monthly Census Summary
- □ Transaction Analysis
- □ Third Party Billing
- □ Resident Master Reports
- □ Resident Trust
- □ RetroActive Billing

Sec. B
Clinical Care (Medical Records) Limited Access

Unchecked boxes will deny access. Checked boxes allows access.

- □ Master File Maintenance**

Assessments:
- □ User Defined Assessments
- □ MDS Processor 2.0
- □ Electronic Submission
- □ MDS Setup
- □ MDS Diagnosis Setup
- □ MDS Logic Setup

Care Plans/Physician Orders:
- □ Care Plan Construction
- □ Edit Care Plan Library
- □ Care Plan Due/Done
- □ Care Plan Assignment Sheets
- □ Physician Orders
- □ Physician Order Print
- □ Transaction Analysis

- □ Resident Master Reports
- □ HCFA Resident Roster (802)
- □ HCFA Census/Condition (672)
- □ Classification Maintenance
- □ Vitals
- □ Resident Trust**
- □ System Maintenance

** Requires Sec. A approval

MDI Access approved by:

Sec A:
Name: _____ (print) Signature & Date: _____

Sec B
Name: _____ (print) Signature & Date: _____

Submit this application to the IT Section once it has been signed by an authorized staff member. Once access has been granted to MDI, the IT Section will meet with the Employee or an authorized staff to provide their password and review the MDI authorized use Policy. Access is granted after the MDI acceptable use policy is understood and signed by the Employee.

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

MDI ACCEPTABLE USE POLICY

(FOR USE ONLY WHEN MDI ACCESS IS REQUIRED)

EFFECTIVE DATE: October 1st, 2003

COPIES OF THIS DOCUMENT ARE FORBIDDEN. KEEP THIS DOCUMENT IN A SAFE AND SECURE PLACE. THE IT SECTION HAS MDI PASSWORDS ON RECORD. For lost or forgotten passwords, call the IT Section (not MDI).

The Arizona Department of Veterans' Services and MDI Technologies operate under HIPAA Privacy and Security requirements. MDI user access has been granted to the above mentioned employee whom accepts responsibility for understanding HIPAA issues and requirements as they pertain to his/her position. In addition, the following security items must be followed at all times:

Never provide your Windows logon, or MDI username and password to another individual. Authorized staff and the IT Section staff excluded.

Never leave your computer unlocked if an MDI session is in use. Log out of MDI if you plan to leave your workstation.

Any unauthorized reading, viewing, copying, printing, or transfer of any MDI data that is not immediately necessary to perform your official duties is prohibited.

Never access or attempt to access MDI information that is not necessary to perform job duties. This includes casual 'browsing' of the MDI information.

Use of your MDI username and password when outside or away from the work place is prohibited. This includes accessing MDI from a personal computer using or allowing a third person or coworker to use your MDI logon session. The IT Section is excluded.

MDI Technologies keeps records of user actions within the MDI database. Any violation of the above guidelines will result in the loss of MDI privileges and will be reported to the administration for disciplinary action.

FOR IT SECTION USE ONLY

Date: _____ Employee: _____

MDI user name: _____

MDI password: _____

ARIZONA DEPARTMENT OF VETERANS' SERVICES

MDI ACCEPTABLE USE POLICY CONSENT FORM

(FOR USE ONLY WHEN MDI ACCESS IS REQUIRED)

EFFECTIVE DATE: October 1st, 2003

COPIES OF THIS DOCUMENT ARE FORBIDDEN. KEEP THIS DOCUMENT IN A SAFE AND SECURE PLACE. THE IT SECTION HAS MDI PASSWORDS ON RECORD. For lost or forgotten passwords, call the IT Section (not MDI).

The Arizona Department of Veterans' Services and MDI Technologies operate under HIPAA Privacy and Security requirements. MDI user access has been granted to the above-mentioned employee whom accepts responsibility for understanding HIPAA issues and requirements as they pertain to his/her position. In addition, the following security items must be followed at all times:

Mark each of the following boxes after carefully reading the respective policy.

□ Never provide your Windows logon, or MDI username and password to another individual. Authorized staff and the IT Section staff excluded.

□ Never leave your computer unlocked if an MDI session is in use. Log out of MDI if you plan to leave your workstation.

□ Any unauthorized reading, viewing, copying, printing, or transfer of any MDI data that is not immediately necessary to perform your official duties is prohibited.

□ Never access or attempt to access MDI information that is not necessary to perform job duties. This includes casual 'browsing' of the MDI information.

□ Use of your MDI username and password when outside or away from the work place is prohibited. This includes accessing MDI from a personal computer using or allowing a third person or coworker to use your MDI logon session. The IT Section is excluded.

MDI Technologies keeps records of user actions within the MDI database. Any violation of the above guidelines will result in the loss of MDI privileges and will be reported to the administration for disciplinary action.

Signature: _____ Date: _____

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

MDI ACCREDITATION

Date:_____

Employee:_____

Approved MDI Trainer:_____

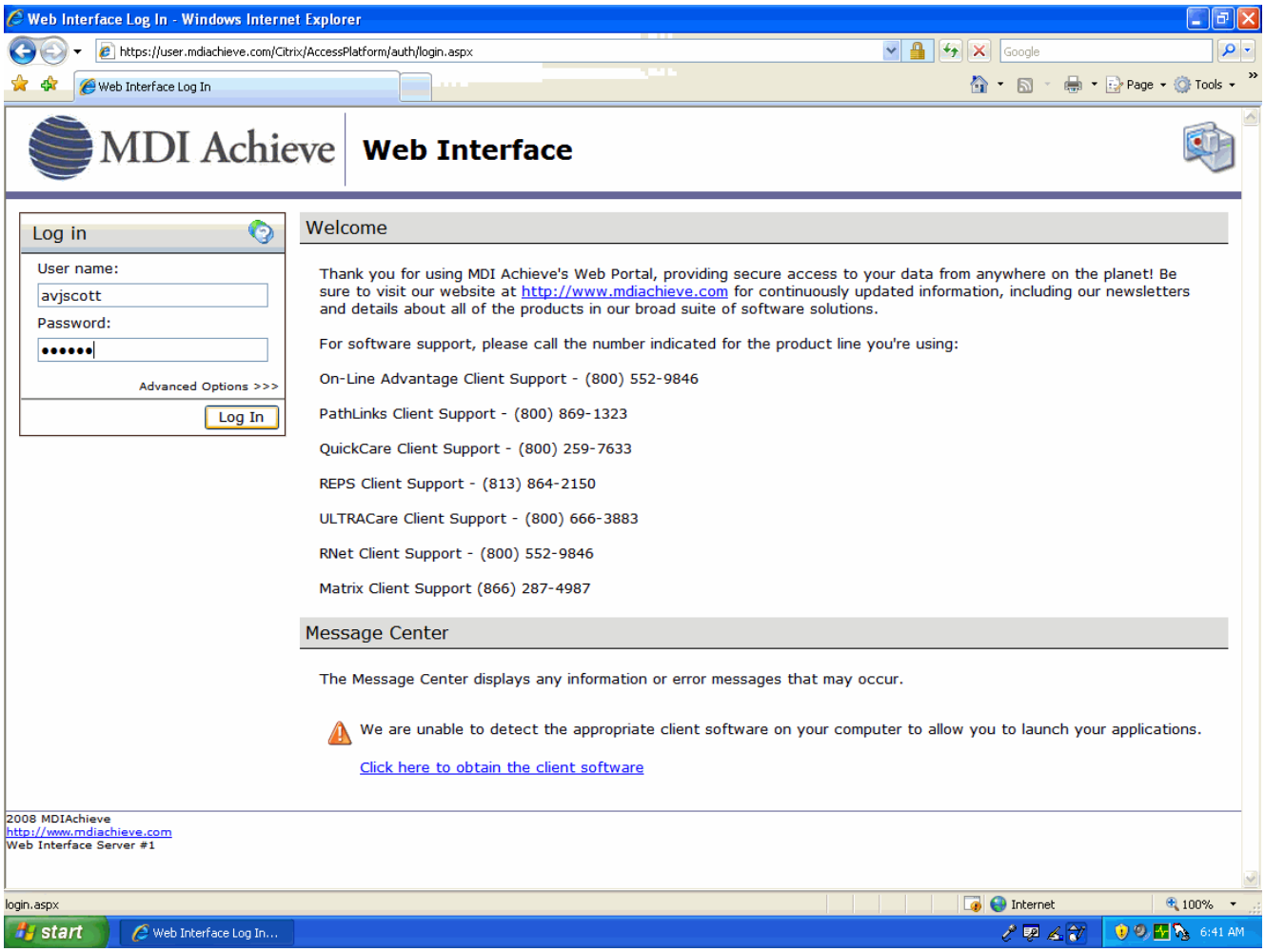
The above stated employee has completed MDI training. The employee understands and has signed the MDI Acceptable Use policy. The employee shall be granted user access to MDI.

_____
Approved MDI Trainer Signature

_____
MDI User Signature

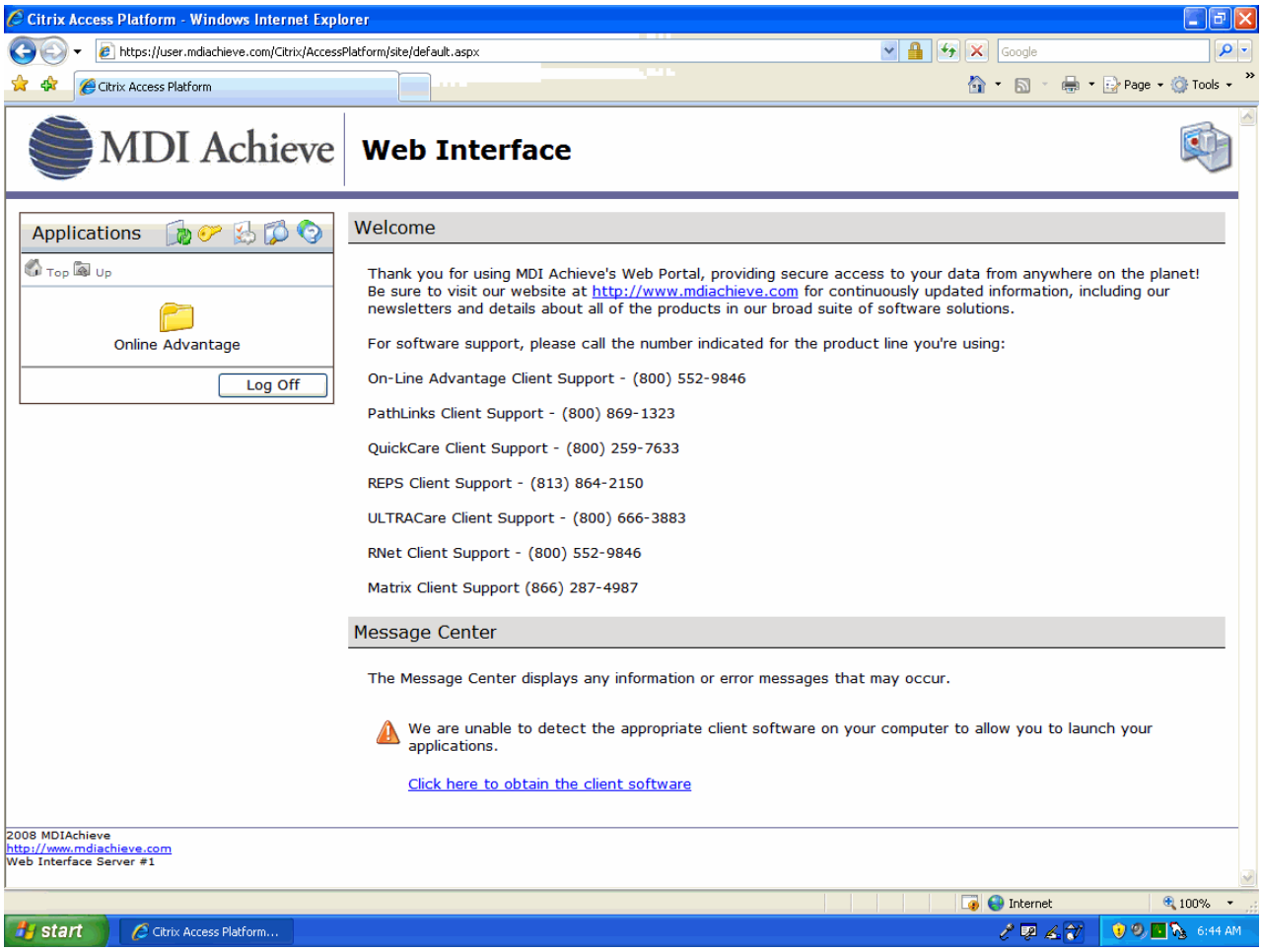
PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

Open you “MDI Achieve” icon and the following screen is displayed
Put in your MDI login and Password then select “Login”



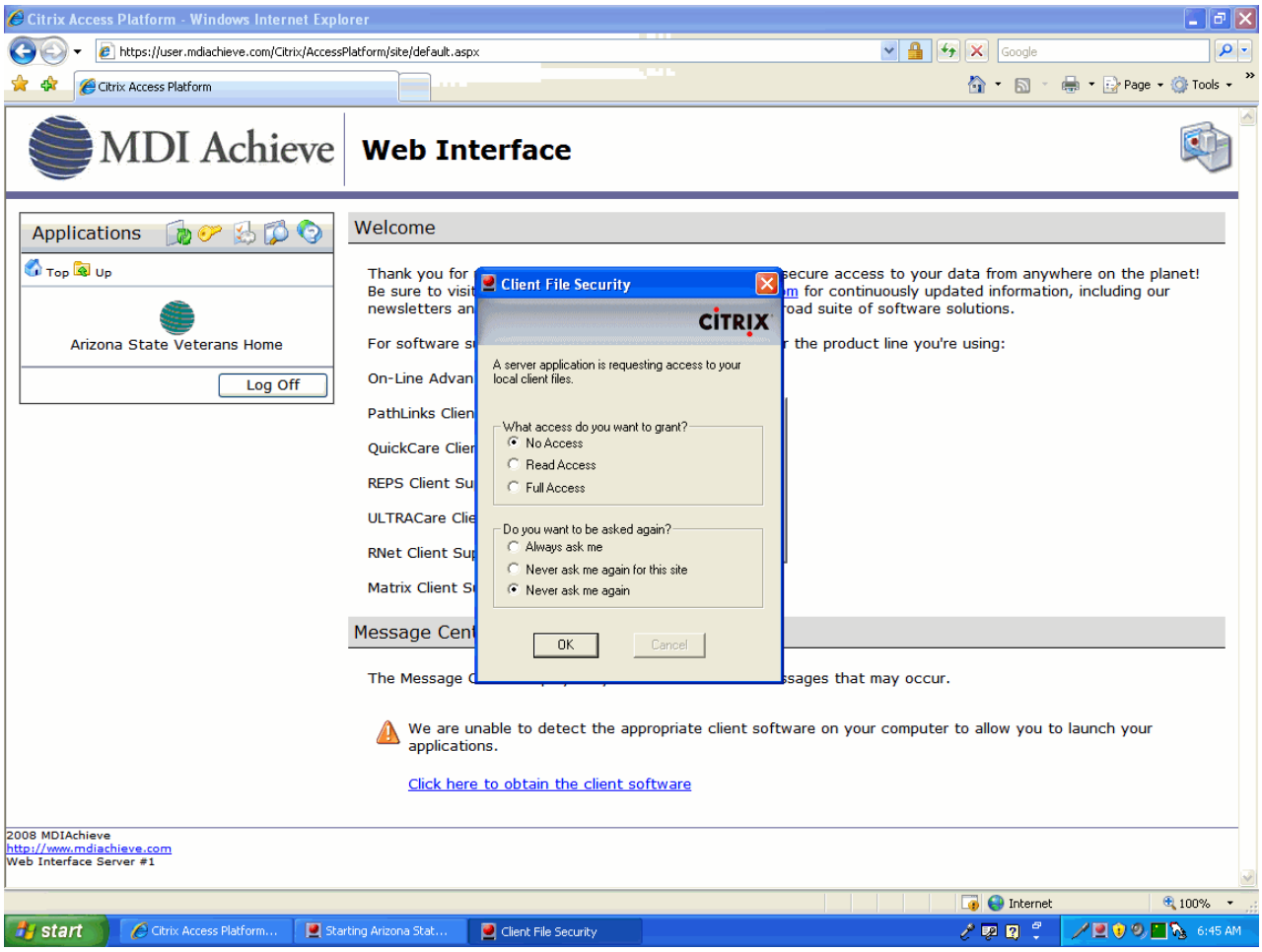
With your mouse, select “Online Advantage”

Note: This screen will usually only appear the first time you use the new login procedures. However if it does pop up when you login again it is not an error, just select it again and move on to the next step.

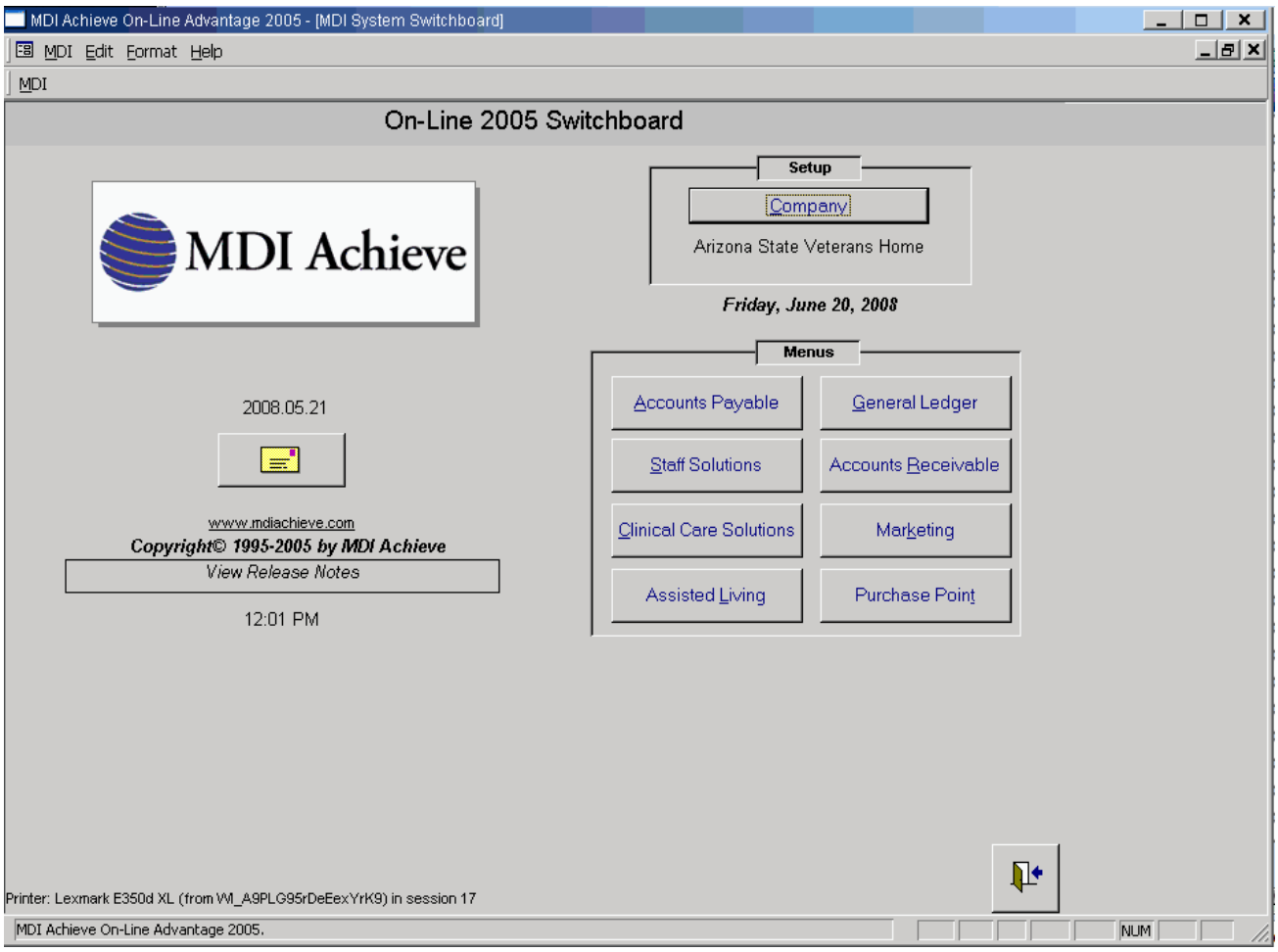


Now mouse select “ Arizona State Veterans Home”

The first time you log in the Citrix “Client File Security” box will appear. Be sure to click on “Never ask me again” before you select “OK”. Checking this item will prevent you from being asked again. Don’t worry if you miss it the first time it will ask you every time you login until you do select it.



You are now logged in and ready to access the various area of MDI.



ARIZONA DEPARTMENT OF VETERANS' SERVICES

VETERANS INFORMATION MANAGEMENT SYSTEMS (VIMS)
ACCEPTABLE USE POLICY
(FOR USE ONLY WHEN VIMS ACCESS IS REQUIRED)

EFFECTIVE DATE: October 1st, 2003

VIMS user name:_____

VIMS password: _____

COPIES OF THIS DOCUMENT ARE FORBIDDEN. KEEP THIS DOCUMENT IN A SAFE AND SECURE PLACE. THE IT SECTION HAS VIMS PASSWORDS ON RECORD. For lost or forgotten passwords, call the IT Section (not VIMS support).

The Arizona Department of Veterans' Services and VIMS Technologies operate under HIPAA Privacy and Security requirements. VIMS user access has been granted to the above-mentioned employee whom accepts responsibility for understanding HIPAA issues and requirements as they pertain to his/her position. In addition, the following security items must be followed at all times:

Never provide your Windows logon, or VIMS username and password to another individual. Authorized staff and the IT Section staff excluded.

Never leave your computer unlocked if an VIMS session is in use. Log out of VIMS if you plan to leave your workstation.

Any unauthorized reading, viewing, copying, printing, or transfer of any VIMS data that is not immediately necessary to perform your official duties is prohibited.

Never access or attempt to access VIMS information that is not necessary to perform job duties. This includes casual 'browsing' of the VIMS information.

Use of your VIMS username and password when outside or away from the work place is prohibited. This includes accessing VIMS from a personal computer using or allowing a third person or coworker to use your VIMS logon session. The IT Section is excluded.

Any violation of the above guidelines will result in the loss of VIMS privileges and will be reported to the administration for disciplinary action.

ARIZONA DEPARTMENT OF VETERANS' SERVICES

VIMS ACCEPTABLE USE POLICY CONSENT FORM
(FOR USE ONLY WHEN VIMS ACCESS IS REQUIRED)

EFFECTIVE DATE: October 1st, 2003

Mark each of the following boxes after carefully reading the respective policy.

□ Never provide your Windows logon, or VIMS username and password to another individual. Authorized staff and the IT Section staff excluded.

□ Never leave your computer unlocked if an VIMS session is in use. Log out of VIMS if you plan to leave your workstation.

□ Any unauthorized reading, viewing, copying, printing, or transfer of any VIMS data that is not immediately necessary to perform your official duties is prohibited.

□ Never access or attempt to access VIMS information that is not necessary to perform job duties. This includes casual 'browsing' of the VIMS information.

□ Use of your VIMS username and password when outside or away from the work place is prohibited. This includes accessing VIMS from a personal computer using or allowing a third person or coworker to use your VIMS logon session. The IT Section is excluded.

I understand and agree to the VIMS Acceptable Use Policy.

Signature: _____ Date: _____

PLEASE SIGN AND RETURN TO:
Arizona Department of Veterans' Services
IT SECTION

ARIZONA DEPARTMENT OF VETERANS' SERVICES

VIMS ACCREDITATION

Date:_____

Employee:_____

VBC III:_____

The above stated employee has completed VIMS training. The employee understands and has signed the VIMS Acceptable Use policy. The employee shall be granted user access to VIMS.

_____
VIMS Trainer Signature

_____
VIMS User Signature